Symbol SECURITY

Creating a Cyber Secure Culture in Your Workplace

Get Your Team Prepared

www.symbolsecurity.com
+1 (973) 381-6077
sales@symbolsecurity.com

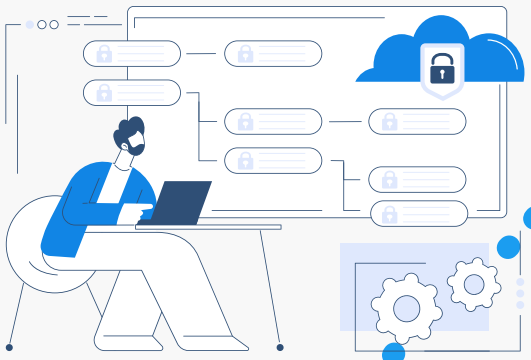
Cyber threats are on the rise faster than you can say "password123," causing significant headaches for businesses big and small. In 2023, the average data breach cost an eye-watering $4.45 million, and a shocking 60% of small businesses hit by a cyber attack fold within six months. These alarming numbers scream the need for a strong cyber secure culture. That's where Symbol Security steps in, offering top-notch security awareness training to keep your organization safe and prepared.

10 Tips for Building a Cyber Secure Culture

1.Leadership Commitment

Lead by Example:
Leadership should demonstrate their commitment to cyber security by actively participating in training and sticking to best practices.

Allocate Resources:
Invest in the necessary tools, training, and resources to maintain strong security measures.



2.Regular Training & Education

Ongoing Education:
Implement continuous training programs to keep employees informed about the latest cyber threats and security practices.

Interactive Learning:
Symbol Security provides engaging training methods to enhance learning, such as simulations, quizzes, and interactive sessions.

3.Internal Communications

Regular Newsletters:
Share regular updates, examples of recent threats, and links to internal resources to keep cyber security top of mind.

Resource Sharing:
Provide easy access to training materials and support resources.

4.Clear Policies & Procedures

Documented Guidelines:
Develop and distribute clear cyber security policies and procedures so everyone understands their roles.

Regular Updates:
Ensure these policies are regularly reviewed and updated to address new threats and organizational changes.

5.Incident Reporting & Open / Anonymous Communication

Non-Punitive Reporting:
Create an environment where employees feel comfortable reporting suspicious activities without fear of retribution.

Feedback Loop:
Establish a feedback loop where employees can suggest improvements and share their experiences.

6.Simulations to Help Sharpen Skills

Phishing Simulations:
Conduct regular phishing simulations to test employee responses and improve their ability to recognize phishing attempts.

Real-World Scenarios:
Use real-world examples to highlight the impact of cyber threats and the importance of vigilance.

7.Take a Lead on Password Management

Mandatory Policies:
Enforce strong password policies, including the use of complex passwords and regular password changes.

Two-Factor Authentication:
Implement two-factor authentication to add an extra layer of security.

8.Clear Remote Work Expectations

Home Office:
Ensure remote workers use VPNs, secure Wi-Fi connections, and follow device management policies.

Road Travel:
Provide guidelines for secure practices while traveling, including the use of secure connections and caution with public Wi-Fi.

9.Data Protection, Privacy & Data Leaks

Handling Procedures:
Implement strict procedures for handling and protecting sensitive information.

Encryption:
Use encryption for sensitive data both in transit and at rest.

Constant Reinforcement:
Regularly remind employees of the guidelines and procedures related to data protection and privacy.

10.Get Proactive about Personal Cybersecurity

Deal with Reality!

- People work from home and on the road, from all kinds of devices and environments.
- Unless your business has mandated a ‘secure office only’ environment, remote work and personal devices are a part of your challenge!

Arm your workforce and Reduce Risk!

- Provide your employees with personal cyber products like **Aura Security**
- Educate on personal and family cyber safety.

Monitor, Review & Adjust

Creating a cyber-secure culture requires ongoing effort and commitment from every organization member. To keep your defenses sharp, it's essential to continuously monitor, review, and adjust your strategies. Regularly check for unusual activity and potential threats, and conduct frequent security audits to identify vulnerabilities and ensure compliance. Continuously assess incidents and monitor employee sentiment to refine your approach.

By embedding these practices into daily operations and emphasizing cyber awareness training, you can significantly reduce cyber threats and maintain a secure environment for your organization.

Symbol SECURITY

About Symbol Security

Symbol Security's SaaS-based phishing simulation and training platform simulates real phishing attacks and reports critical data and trends back to authorized administrators. Symbol can be operated by company administrators with ease, or leveraged by Managed Security Service Providers as part of their security offerings.

Get in Touch

115 US Highway 46, Building F,
Mountain Lakes, New Jersey, 07046, USA

www.symbolsecurity.com

+1 (973) 381-6077

sales@symbolsecurity.com

company/symbolsecurity

Symbol_Security